Date: February 13, 2008

To: JPAMidTermReview@ntia.doc.gov

Susan R. Sene
Office of International Affairs
National Telecommunications and Information Administration
1401 Constitution Avenue, NW., Room 4701,
Washington, DC 20230
USA

Subject: Midterm Review of the JPA, comment "The Miner's Canary in ICANN Governance"

From: Thierry Moreau
thierry.moreau@connotech.com

CONNOTECH Experts-conseils, inc.
9130 Place de Montgolfier
Montreal, Qc
Canada H2M 2A1

Tel.: (514)385-5691

Dear Ms Sene:

In response to the NTIA Notice of Inquiry on "The Continued Transition of [...] the Joint Project Agreement", I submit the following contribution.

Thanks for handling these matters.

Best Regards,

Thierry Moreau

The Miner's Canary in ICANN Governance

by Thierry Moreau

February 13, 2008

Reply to the Notice of Inquiry
on
"The Continued Transition of the Technical Coordination and Management
of
the Internet's Domain Name and Addressing System:
Midterm Review of the Joint Project Agreement"

First, I would like to thank the US government NTIA department of commerce for the opportunity to comment on the ICANN progress towards the JPA goals.

This comment will focus on the implementation of DNSSEC for the DNS root zone file. On one hand, this is a small piece in the wide range of ICANN areas of involvement for which the various stakeholders have great expectations, e.g, IDN, IPv6, new gTLD introduction processes, price regulation of the wholesale gTLD registration market, DNS root nameservice, UDRP, and the like. On the other hand, DNSSEC changes something at the DNS root, maybe very little fundamentally but nonetheless in an area where the "U.S. Principles on the Internet's Domain Name and Addressing System" are most specific: the US government will "maintain its historic role in authorizing changes or modifications to the authoritative root zone file. Thus, the fate of further DNSSEC deployment progress is like a miner's canary in the field of US government oversight of ICANN activities (referring to the use of canary birds used in coal mines for early warning of dangerous gases): lack of progress would be an early sign that the US government is committed to continued oversight.

The timing of the NTIA notice of inquiry is such that I can report clear signs of progress within the IANA function at ICANN towards an acceptable technological and organizational framework for DNSSEC support at the root. The remaining of this comment attempts to describe in simple terms how a specific aspect of DNSSEC, cryptographic key management, may interfere

with the above US principles citation. The conclusion is straightforward.

DNSSEC affixes cryptography-based integrity marks to DNS responses originating from authoritative nameservers. If and when the DNSSEC support is added to the authoritative root zone file, the DNS root servers will thus provide an integrity-protected publication mechanism for the IANA maintained root zone. Although the integrity marks are "public key digital signatures," DNSSEC purpose is limited to preventing tampering of DNS data on the fly (from the authoritative nameservers to the end-user), and comes with no additional assurance that an authoritative zone file contents was proper by any criteria. The very desirability of DNSSEC as a public service is subject to debates over its effectiveness as a security incident countermeasure and the intrinsic complexity of the protocols. For the purpose of this comment, the niche applications that would be strengthened by a better integrity in the DNS are deemed sufficient justification for DNSSEC support at the root.

Given the hierarchical structure of the DNS and the operating principles of digital signatures, DNSSEC overall deployment requires a "DNS root key" which becomes a system-wide master key. The criticalness of this cryptographic key comes from the Internet-wide re-configuration that would be required it the key is compromised in a security incident, with a significant impact on IANA and ICANN public standing as reputable organizations (such a security incident would be caused by a breach of secrecy for the *private counterpart* of the DNS root *public* key).

In summary, from the definition of DNSSEC and the observation of the criticalness of the DNS root key, I can introduce the topic of cryptographic key management applied to the ICANN oversight by the US government. There are two aspects of cryptographic key management relevant to system-wide keys like the DNS root key, and any "power" over the DNS granted by the control of this key is *not* among them. At most, the DNS root key could be argued to grant some special status to its controlling entity – a status which, I believe, ICANN already has. In fact, the control of the DNS root is a mere requirement for the provision of DNSSEC integrity service to the Internet.

The two relevant aspects of cryptographic key management are more prosaic, namely 1º the long life span of the DNS root key (I am actually referring to the continuity of DNS root keys periodically rolled by the controlling entity – such trust anchor key rollover is of secondary relevance for the purpose of this comment), and 2º the almost certain recourse to split-knowledge storage technique for the private counterpart of DNS root key(s).

The long life span of the DNS root keys makes the DNSSEC deployment endeavor a much longer-term activity than the IANA contract duration. For sake of focus and clarity, I do not discuss the governance implications of the long life span of DNS root keys.

In modern IT security techniques, the split-knowledge storage technique finds a very narrow field of application, yet a critical one, for system-wide master keys. If one makes a scholarly study of certification schemes for cryptography-based IT security techniques, e.g. studying both the NIST-specific USG procurement specifications (FIPS140-2) and the relevant protection profile documents drafted according to the multi-national "Common Criteria," it becomes clear that the split-knowledge storage technique is relevant for system-wide master keys used in any cryptographic scheme operated as a public service, such as DNSSEC support at the root.

With the split-knowledge storage technique, the secret associated with the system-wide master key is split among a small number (say 2 to 5 in practice) of *key custodians*, and the recovery of the secret requires the coordinated participation of these custodians (there are fail-safe variations of the basic scheme which are of secondary relevance for the purpose of this comment).

This leads to this simple question: who will be the key custodians in the specific split-knowledge storage scheme to be selected for DNS root keys? Obviously, the issue is less the very question than its impact on ICANN governance.

A first approach is to deny any link between such a minute technical aspect, and governance. In this view, the security technology suppliers and managers will address the split-

knowledge storage requirements. Indeed, I checked that, as expected, the HSM (Hardware Security Module) product line in use at IANA in the DNSSEC test environment supports split-knowledge storage of master local keys (which translates into control f the DNS root private key according to the detailed key management scheme). However, I have yet to see a written proposition for allocation of the DNS root key custodian responsibilities, with a claim that the proposed allocation meets the accountability and transparency expectations applicable to IANA.

A second approach is a statement that the IANA "organization" is empowered to handle key custodianship by itself, wholly within the limits of its mandate. This is similar to the preceding approach, with an explicit endorsement by the institutions on the governance side of the equation. Actually, the data escrow arrangements that protects the USG against a collapse of IANA may be extended, perhaps with minor amendment, to cover the secret data kept by the DNS root key custodians. This approach is straightforward and seems to be the default. However, the IANA organization becomes a single point of failure, and a fairly visible one with the transparency expectations for DNS root management. Such visibility should be manageable, somehow.

From the preceding observations about the much longer life span of DNS root keys compared to IANA contract renewal and about the DNS root key management as a single point of failure, I formalized a refinement of DNSSEC key management for the root with a two-tier key management scheme ([1]). Only the higher tier has a requirement for the split-knowledge storage technique. The lower tier is the DNS root zone operation; a key compromise or an organizational collapse at this tier is recovered by the higher tier. The proposal thus mitigate the single point of failure issue, and would be applicable with either the above second approach, or the next one.

The third approach encompasses attempts to spread the allocation of the DNS root key custodian responsibilities across institutional oversight boundaries. It is certainly very challenging to formulate any such concrete proposition since it must explicitly cover ICANN oversight aspects which are dormant in the contractual history and bargaining forces that shaped the current and moving institutional arrangements. In this respect, the two-tiered key management scheme is slightly more than a mere technological proposition: its potential to mitigate the single point of failure issue rests on defined roles. However, a convincing proposal encompassing the

technological and institutional perspectives is yet to be cited (with or without the two-tier concept). A DHS study circulated in October 2006 downplayed the split-knowledge storage technique and accordingly disqualified itself by any realistically applicable security certification standard, and contained implicit institutional suggestions that triggered loudly voiced questioning.

In summary, the above explains how DNSSEC deployment at the root organismically operates like a miner's canary in the ICANN governance field. DNSSEC is a relatively minor challenge to ICANN, yet with strong bind to the USG oversight of ICANN and IANA. In an optimistic conclusion, let me assume the canary remaining healthy, i.e. the USG steadily making progress towards ICANN independence. The logical conclusion is to recommend the straightforward approach of letting IANA arrange DNSSEC deployment at the root with minimal ties to the USG as the ICANN overseeing organization. In any event, until the US Principles on the DNS are retracted or amended, it seems that only USG can indicate the way forward.

Reference:

[1] "A (Pro?-)Position Paper re DNS Root Zone File Signature Using DNSSEC Protocols" available at http://www.connotech.com/dnssec_root_ta_takrem_v1.pdf

- * - * - * -